On BlockChain Technology: Overview of Bitcoin and Future Insights

Hussein Hellani
Saint Joseph Univeristy
Lebanon, Beirut
Hussein.helani@cci-me.com.lb

Abed Ellatif Samhat
Lebanese University
Lebanon, Beirut
samhat@ul.edu.lb

Maroun Chamoun
Saint Joseph Univeristy
Lebanon, Beirut
Maroun.chamoun@usj.edu.lb

Hussein El Ghor
Lebanese University
Lebanon, Beirut
husseinelghor@ul.edu.lb

Ahmed Serhrouchni
Telecom ParisTech
Paris, France
as@telecom-paristech.fr

***Abstract*— In this paper, we consider blockchain technology that enabled the existence of digital currency and we investigate Bitcoin cryptocurrency application. This technology nowadays represents a new feature that replaces existing client-server core system on top of some distributed systems with many additional features such as high availability, resistance to alteration, fault tolerance and cost reduction. After overviewing how such technology is working, we highlightthe requirements and benefits related to the security, database and network. We mainly focus on answering the most Bitcoin queries including privacy and double spending. Furthermore, as blockchain has potential applications far beyond bitcoin, we draw future insights where applications based blockchain are provisioned in the market in order to be totally or partially independent of the centralized systems and we provide a questionnaire helping organizations for better using the blockchain feasibilities.**

Keywords: POW; Blockchain; P2P; distributed ledger; Consensus.

I. INTRODUCTION

Contrary to the days of old, we're now experiencing a fast paced boom in technology. Within the past few years, the services' consumption and how enterprises provided these servers were subject to a lot of changes. these changes haven't stopped and the market demands high modularity when it comes to its need. It is obvious that a true replacement of the old technologies has occurred during the past few years and the slow computing machines do no longer exist. Thanks to this progress, the world now witnesses a rapid development in both hardware and software fields and new concepts and models appear with direct impact on our daily jobs, tasks and achievements. Nowadays business applications are based on a centralized data center consisting of many physical servers located basically in one or more place, offering application services to their employees/clients across many regions, reliant significantly on the internet service. Installing applications on these servers came later with a notion of high availability “HA” such as VMware fault tolerance, Microsoft exchange data availability group “DAG” and no later SQL Always-on, to eliminate single point of failure in case of disaster. “HA” is a server role, aims to distribute an application and/or database to different server nodes to provide always on services. This feature is applied by integrating what is called “Quorum” [1] or witness file in order to vote for which server(s) should be active at any given time. Beside the centralized revolution, a newly decentralized system called Blockchain [2] imposing itself on the scene to eliminate the concept of third party existence. This is achieved by supposing new different architecture whereas databases are distributed across the whole participants of the network, similar to the server redundancy but in a very high scalability and independent of any kind of central control. With centralized systems such as those existing in the banking sector, all data and applications are monitored by their owners (whom are few) and thus any transaction that is triggered by a client must be verified by one of the application owners and this effectively makes it costly from both a time and fees perspective. With Blockchain technology, each participant *is the Bank* compared to the up-to-date copy possession. Blockchain revolution changed the owner authority fundamentally. It came with four main basic features: *decentralization*, *distributed*, *immutable*- hence data cannot be changed without leaving a trace, and *transparent* where participants rely upon each other to compute transactions. This new technology is mainly based on hash functions, asymmetric key pair cryptography and digital signature.

Thus blockchain is a technology that provides a distributed ledger of transactions on a network that is scalable, secure, tamper-proof, and accessible by each peer on the network. It is shared transactions, distributed over a network of members, made up of series of data blocks, each by itself contains a set of transactions. Blocks are electronically chained together and locked with cryptography, and a public record of every transaction is established. The more blocks there are, the less the probability that blocks can be altered. The well-known cryptocurrency for which blockchain technology was invented is the Bitcoin, invented by Satoshi Nakamoto in 2008 [2]. In intelligent way, Nakamoto combines the previous technologies of security: Hashcash [3], asymmetric encryption, consensus [4] and Merkle tree [5] to invent what is called bitcoin cryptocurrency. Officially, the first block (genesis) was initiated on 2009, thereafter the chain is increasing every few minutes to reach around 52k blocks on year 2018 with BTC price growing up to 8k$ for each bitcoin.

The success of bitcoin triggered the technologists to think of decentralization and start researching about the topic. It is important to distinguish between bitcoin and Blockchain, where bitcoin is an electronic cryptocurrency that can be used to purchase goods or services based on incentivizing the participant nodes (miners), to validate transactions and to render the network as stable as maximum. Blockchain is the underlying technology that enables the Bitcoin network to operate in an open, autonomous, decentralized model, where trust is enforced through cryptography and not over its

978-1-5386-4500-0/18/$31.00 ©2018 IEEE

participants. Essentially, there would be no bitcoin without Blockchain, but there can certainly be Blockchain without bitcoin. This distinction is significant because blockchain technology can be applied to other uses rather than financial development. In this paper, we consider blockchain technology and we investigate Bitcoin cryptocurrency application. We draw attention to bitcoin functionality in general and the problems/solutions of that technology in specific.

The rest of this paper is structured as followings: in section II, we will explain in details the Blockchain behaviors in terms of bitcoin. In section III, we will focus on the underlying bitcoin queries and available solutions. Section IV, discusses the future of blockchain apart from bitcoin technology, and we conclude in section V.

II. BLOCKCHAIN PHENOMENON

Many questions arise when talking about decentralization and the new technology version which should replace an existing client-server core system. Concerns are many in such major turning point, mainly the network stability, security threats, power of consensus and participants' privacy. To address these queries and more, we should first present the most famous use case "bitcoin", as it is the originator of Blockchain and it will be a good starting point towards generalizing the decentralization system that is already the hot topic of the newest generation of technology.

A. Understand Bitcoin

Bitcoin word denotes three different objects: *Blockchain platform*, *digital currency, and protocol* that runs over this platform to define how transactions are moved. Bitcoin was invented in 2008 with the publication of a document entitled "Bitcoin: A peer-to-peer electronic cash system" written under the pseudonym of Satoshi Nakamoto. He has combined several previous inventions such as b-money and Hashcash [3] and existing contributions from decade of research [6], [7], [8] to create a completely decentralized electronic cash system that does not rely on any central authority for issuing currency or validating transactions. The main innovation is to use a distributed computing system (known as a "proof-of-work" algorithm).

After the failure of precedent trials such as [9], [10], Bitcoin answers the big query which was raised many years ago: how can we eliminate the bank and force P2P transactions? The answer of Nakamoto proposal was simply: it is analogous to "everyone is the bank", where most participants keep a copy of the data which would be the bank responsibility. This data called "distributed ledger" contains all preceding and current transactions. Now the sender and the receiver are totally independent of any kind of third party control. On the other hand, they are submitted to a new network control called "consensus" that accepts or refuse their transaction(s) based on a ledger content. Using "consensus", majority of the network users vote for transactions to be passed or blocked. Bitcoin is a fully distributed peer-to-peer system. Thus, there is no dominant server or single point of control system; in contrast, bitcoins are created through a process called "mining", which is involved in the procedure of finding the solution of difficult problem. Any participant in the bitcoin network (any computer operating the complete bitcoin stack) can act as a miner, using the computing power it has at its disposal in order to solve the problem. Every 10 minutes in average, a new solution is found by someone who is then able to validate the transactions of the current block. In summary, bitcoin mining decentralizes the issuance of money and reconciles the different procedures, making unnecessary for a similar body to act as a central bank. The participants (nodes) that are spanning across different regions and countries interconnect in a mesh network with a "flat" topology. There are two types of nodes: mining nodes are the users who participate in the creation of blocks and are incentivized by an amount of bitcoin to guarantee their presence in the network. The non-miners benefit from the bitcoin system without participating in the block creation. The second main role of this incentive is to issue the Bitcoins currency, started by 50BTC for each block (every 10 minutes) at its launch on 2009 and is being halved every 4 years to reach around 21billion BTC on 2140. By year 2032 the incentive will be less than 1 BTC, at that time incentives shall be replaced by the transaction fees only. The future of fees is not clear after year 2140 where incentive will no longer exist [11].

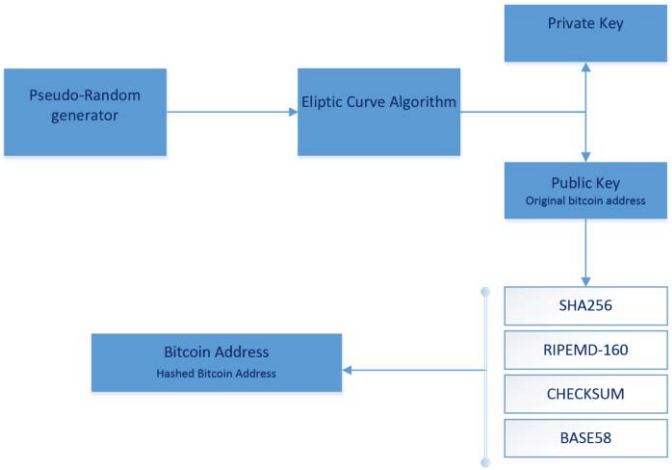

Figure 1: Bitcoin address construction

The three main core components of bitcoins are:

1- Transactions and scripts

2- Consensus and mining

3- Peer to peer communication network

In details, the transaction is mainly based on a public /private key pair and hash functions, where transactions are signed and distributed on a public network. Public and private keys are referred to asymmetric cryptography, so they are mathematically bounded and cannot be interchanged. In other words, the public key only functions with its corresponding private key. Transactions are then grouped into blocks, shared and validated by a network of nodes, wherefore Consensus on the network determines which blocks are accepted. To generate the Bitcoin address, SHA256 and RIPEMD-160 hashing functions are first applied to the public key as shown in figure

1. A network identifier is added to the front of the address to identify which network the address is intended for, then a checksum is appended to the end of the address. Finally, a BASE58 function is applied to the string of network identifier, hash and checksum to encode large numeric values into an alphanumeric string of characters. The BASE58 output can be easily read or written by humans, making it useful for creating Bitcoin public addresses.

Every user in the bitcoin network has a virtual wallet consisting at least of one public/private key pair. A new key and address are recommended for each transaction to avoid comparison-based attacks on signatures [12] and tracking of coin flows [13],[14]. Each wallet contains a list of inputs and outputs in order to receive and send coins via transactions. Each output of a transaction can only be used once as an input in the whole blockchain, otherwise using the same output twice it will be considered as an attempt for double spending, thus forbidden. Accordingly, the output of a transaction is categorized by either unspent transaction output (UTXO) or spent transaction output (STXO). Each input of a Bitcoin transaction connects to a given, previous output, thus transactions between two users pass from sender input to receiver output. In fact there is no user balances, instead, there is only set of UTXO scattered in the blockchain ledger. So, a user who intends to send bitcoin to someone else, must consume the entire UTXO amount and produce two outputs: one for paying the desired bitcoin to a specific recipient address and another for paying the change back to the sender wallet. Since wallet is designed to contain many addresses, a user who receives many payments from different senders in separate time, will have a wallet containing addresses from each sender with the specific amount of bitcoins. To clarify, assume that Alice received 2 BTC from Jean, 5 BTC from Charlie and 1 BTC from Micheal. She needs to send Bob 1.5 BTC for some online service. None of her addresses adds up that amount even when combined. Alice then will send the 2 BTC received from Jean input to Bob output using her private key to sign the message. So, her wallet will automatically create two outputs for her transaction: 1.5 BTC to Bob, and 0.5 BTC to a new address, which is created for herself to get the change from Bob.

A set of scripts is settled to accomplish a secure bitcoin transfer between two or more untrusted parties as illustrated in figure 2: *P2PKH* (pay to public key hash) means pay to a specific bitcoin address. It is an instruction on the blockchain to transfer ownership from a current owner to a new one of the bitcoin address. A receiver should create a private/public key pair, hash its public key and send the hashed key (receiver's address) to the sender in the first step. Then the sender creates a new transaction with a specific amount addressed to the hashed public key address of the intended receiver. After that, the sender broadcasts the transaction he created to the blockchain network that will be categorized as UTXO for the receiver's wallet after being verified by the network nodes. Later, when the receiver want to spend this amount, he should first create a signature script called *scriptsig* to prove that he is the owner of these bitcoins. This procedure can be done using his unhashed public key: it firstly hashes the same value as the sender provided during P2PKH, then using the ECDSA cryptographic formula lets the pubkey script verify that he owns the private key which created the public key. This transaction behavior lets the receivers prove their ownership as well as it makes broadcasting over a network safe and tamper-proof.

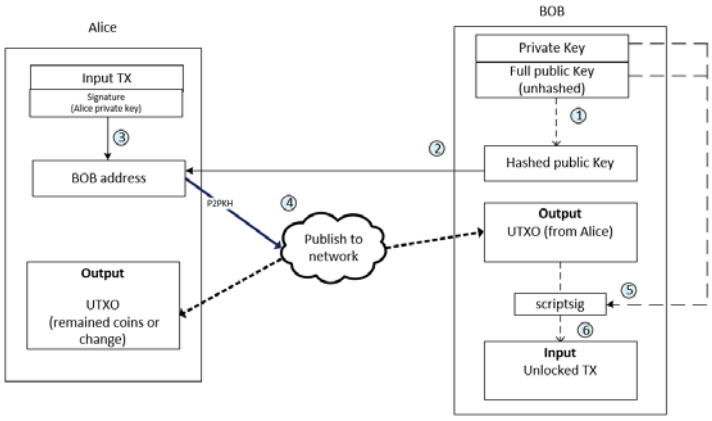

Figure 2: Spending P2PKH output

Another script has been added in 2012 called pay-to-script-hash *P2SH* [15] to replace pubkey script by redeem script. A redeem script is created by the spender, it is hashed and pushed to sender same as pubkey. To spend the output, spender provides his signature along with the full redeem script in the signature script. The bitcoin network ensures the full redeem script hashes to the same value as the script hash sender put in his output; it then processes the redeem script exactly as it would if it was the primary pubkey script.

All transactions are continuously passed to miners for verification in a peer to peer network. The miners are individuals or groups, pool, running the bitcoin software in a worldwide network of independent computers. They compete to turn the latest transactions into a block. Roughly every ten minutes, one of them succeeds. This process is called “Proof-of-work” which is considered as the main bitcoin component against denial of service and Sybil attack [16]. Proof-of-work in short consists of calculating a hash of the formed block and adjusting a nonce in such a way that the hash value is lower than or equal to a certain target value. A reward is delivered to the miner that solves the puzzle for two reasons: network stability that motivate the participants to stay online, and to issue bitcoins. Currently reward is 12.5 BTC for every puzzle solved and thereby a block is added to the chain. Beside, these purposes used to maintain a waiting time of 10 minutes between two successive blocks. Every two weeks (2016 blocks), a target is readjusted to meet a verification rate of approximately one block every 10 minutes. The new target T is given by:

$$T = T_{\text{Prev}} \bullet t_{\text{actual}} \div (2016 \bullet 10 \text{ min})$$

t_{actual} is the time taken to issue 2016 blocks using T_{Prev} the previous target. If those 2016 blocks were produced during a time frame shorter than two weeks, this means that the computing power has been increased by miners, and the proof of work difficulty should be increased to maintain the 10 minutes of block creation and vice versa.

III. BLOCKCHAIN QUERIES AND ANSWERS

The easiest way to study the blockchain model is to pass through bitcoin characteristics and topology in order to address its strengths and weaknesses. In this section we will focus on answering the most bitcoin queries.

A. Distributed ledger control

Blockchain network is a peer to peer network (P2P) relying on consensus concept and proof of work. By comparison to centralized systems where data is stored in a huge storage that is redundant, backed up and probably safe, blockchain database is located on a normal computer running perhaps on a single data drive. Each node of the P2P network keeps a copy of the database that contains all the transactions which are above 100GB. Thereby such blockchain mechanism impedes the participation of small device capacity such as mobile and IoT devices. Nakamoto solved the reclaiming disk space using Merkle tree [5] where transactions are hashed according to a tree of hashes with only the root included in the block's hash instead of storing the whole hashed transactions. With referring to [29], big data is the future of blockchain to mitigate the risk of huge data, as it is already used by many distributed databases such as google, facebook, and others.

B. Wallet Protection

Each bitcoin user has a wallet that is composed mainly of private/public key pair. Since these addresses represent direct money or they are the bank themselves, then it is highly necessary to protect them against exploitations. In bitcoin, there is a variety of wallet types with different level of security, such as software, hardware, paper, brain and online wallets as shown in figure 3. Both software and online wallets are exposed to attackers since they are connected directly to the internet, hence an attacker can gain access to the entire machine and steal their wallets' addresses. The main idea is to protect the private key from being lost, because losing access or account usage by any non-owner users is equivalent to losing bitcoins. Hardware wallet is a new invention to hide sensitive operations throughout a hardware token that delegates the creation of transactions to another entity and allows independent review of transaction details before signing, this taken called bluewallet [17]. In addition, there are also traditional ways to protect private keys either by storing the key on a physical document called paper wallet, or store it in the user's brain called brain wallet.

The most important method to secure online wallets is m-of-n multi signature transactions [18] used within P2SH method, and based on providing m valid out of n possible signatures to redeem a transaction. Only the recipient who created the P2SH address knows the full redeem script. This method is used mainly to dispute mediator so coins are locked and neither the receiver nor the sender alone can claim them. If, however, both agree, the sender could pass a half-signed transaction over to the receiver, who is now able to complete the transaction. A very similar method to multi signature is the threshold signature [19],[20] characterized by its main property that the key is never revealed, so trusted user should provide a subset equal to or greater than a predefined threshold to be able to reconstruct the private key.

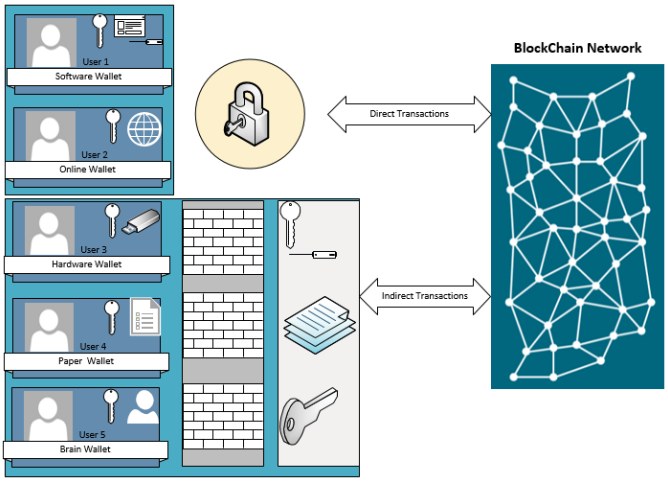

Figure 3: Blockchain wallets types

In addition, bitcoin makes use of elliptic curve cryptography [21], [22] to prove user's ownership. Thereby he needs to provide his public key and signature whenever he participates in a new transaction. Furthermore, many applications use multi factor of authentication to protect their users from losing their accounts. It is based on "something you know (private key or password) and something you have (email, mobile, etc..) to make the hacker mission difficult as a much as possible.

C. "Double spending" meaning in P2P network

Double spending means that someone can issue more than one transaction in parallel and transfer the same amount to different recipients. In a centralized bank system, double spending has been resolved permanently by assigning a serial number to each transaction and thereby ability to detect such suspicious behavior. But with P2P network concept, where the third party is totally eliminated and some participants might be malicious, it ought to be taken into consideration to resolve it as it is considered the highest risk factor that hinders blockchain expansion. In general, with bitcoin P2P network, double spending is almost blockaded by enforcing a rule during transaction propagation and mining. As per this rule, only previous unspent transaction outputs may be used in the input of a current transaction. Moreover, transactions' order within the ledger, replaces the serial numbers used by a centralized system. On the other hand, the distributed ledger which is in a continuous synchronization across a large network scale, is vulnerable to Sybil attack [16] by relying on redundant operations to defeat the consensus mechanism. In a Sybil attack a single node is presented illegally to other nodes in the network as multiple nodes. This attack is feasible by either faking new identities, or stealing legal identities. This type of attack is resolved by bitcoin proof of work thus the attacker capabilities become limited by his/her computing power. As the network grows up quickly, resulting some blockchain fork(s) due to more than miners solve the difficulty of power of work "POW", thereby an adversary can exploit such scenario to perform double spending attacks. Under the condition of synchronous communication, bitcoin network is resilient to adversaries controlling less than half of the computational power, relying on byzantine resilience [23] where the honest nodes n prevail the adversaries f by the ratio of $n > 2f + 1$.

This inequality defined by [23], guarantees system stability in presence of limited adversaries.

Adversary can secretly mine on a fork which builds on the last block, includes double spending transaction. If adversary has chance to solve the proof of work, he will add a new block to the blockchain containing conflict transactions. This attack is known by finney attack [24]. Bitcoin developers enforced the six blocks confirmation to avoid such attack, where a block is considered valid after six confirmations, giving enough time to other nodes to verify the transactions. However double spending cannot be eliminated completely and is still possible for an attacker earn more than 50% of the computational power, which is the worst case scenario, known by 51% attack or *goldfinger attack* [30], that definitely lead to success.

D. Reach consensus in P2P network

The ideal network scenario within bitcoin P2P network is to propagate transactions as fast as possible to reach consensus and build a blockchain. Thereby the rule of thumb is to reach distributed consensus so nodes agree on the value which is generated by the honest node only. A large networking company such as Facebook, Google have thousands of servers distributed across many regions, each information should be recorded and replicated to other nodes instantly. The main difference in bitcoin is that transactions are put into blocks where consensus is applied on a block-by-block basis. Each node in the P2P network has a copy of ledger consisting of a sequence of blocks, each of them containing the valid transactions that was agreed on. In addition a node has multi transactions that are in progress and waiting to be included in the next block. Transactions that are not included in the block due to network latency, they will be included into the next block. Bitcoin protocol is designed to achieve consensus under two main obstacles: imperfection of the network such as latency since the nodes are connected through internet, and presence of malicious nodes that attempt to subvert the consensus process. One of the much known concerns is byzantine general problem [23]. Inspired from byzantine army where their groups of lieutenants were commanded by one general to attack or suspend and were communicating via messenger. In case generals or lieutenants could be traitors thus they attempt to subvert the process in order to avoid the loyal generals to arrive at a unified plan. It has been proven that this is impossible to be achieved if one-third or more of the generals are traitors. An alternative consensus algorithm called Paxos [25], initiated on 1989, integrates fault tolerance in a distributed database consensus-based but it is still not applied due to its high processing requirement (digital signing) and communication (decisions cannot be made based on simple majorities).

Despite all the negative results were proven in a specific model, the surprise is that bitcoin consensus is working better in practical rather than theoretical, due to the incentive released within each block that push the nodes to behave honestly. But it is still mandatory to go deeply into research to identify how exactly this consensus is working to avoid any misbehaviors in the future.

Beside transactions and scripts, consensus mechanism is considered the main core of the P2P bitcoin network within the total elimination of the bank. Thereby, network stability and performance have a direct impact on consensus protocol since latency between the discovery of a block and its receipt by all other nodes could lead to a temporary fork. In addition, network latency could increase the possibility to win a block by malicious miners who are able to control a substantial portion of the network by broadcasting their own blocks. Therefore, it is necessary a decentralized system to propagate their message in a low latency network in order to render the attacker mission as difficult as possible. By design, each node in the network aims to connect to its neighbor nodes through eight minimum connections and 125 maximums. A node connection is made of application handshake and a message including timestamp, IP addresses and protocol version, thereafter each node maintains a list of known peer addresses. The act of nodes to keep asking continuously each other about their network lists that contain peers of different areas, can limit an attacker of controlling its neighbor's environment. Peer keeps sending messages in a continuous manner every 30 minutes to prove its availability in the network, thereby in case a peer doesn't send any message within 90 minutes, thus a heartbeat message is broadcasted telling that this peer does no longer exist in the network. In details, a sender who prepared its transaction including information about input and output sends an inventory message (including TXIDs hashes only) to all its neighbors he/she wants to broadcast a data message on the network. Then the neighbors ask the sender to send its transaction for verification then broadcast it to all the neighbors to be included in the next block. In case the transaction doesn't get into blockchain, the originator is responsible to retransmit it.

E. Privacy: Identity protection

As bitcoin is a P2P distributed system, thereby the full nodes are able to see the entire transactions history including balance details of every account in the system. An account consists of a hash over public key referred to the bitcoin address of the intended participant, who's able to have more than one address under his wallet. Bitcoin address is not anonymous, but, rather, pseudo-anonymous. Anonymity means that someone's identity is completely unknown. Any act made by an anonymous person cannot be associated with the individual who actually made them. On the other hand, Pseudonymous means that a real name isn't used to identify the user. In bitcoin, the hashed public key is the replacement of the participant's identity. Thus, to transfer an amount of bitcoin from Alice to Bob, she first needs to create a transaction include the specific amount together with the hashed public key of Bob and propagate it to the network after being signed by her private key. The message is then published by Alice, so every participant in the network can detect that Alice's account is minimized by n amount of bitcoin and Bob has additional n bitcoin in his account. In order to spend this amount, Bob create a transaction to verify his ownership of the UTXO. An attacker attempts to discover the user's identity by mapping between users and public keys, but the bitcoin is structured to frustrate such breaches by storing the mapping of

a user's public-keys locally on its node only and by allowing each user to generate as many public-keys as required [26].

IV. FUTURE INSIGHTS

As of 2008, the blockchain technology has emerged into our daily life and the big change began. Obviously, this new technology has a global presence nowadays, thereby the blockchain concept becomes more mature by the time. Enhancements over bitcoin application, made it explode into mainstream hence bitcoin is going to be a legal currency as in Russia and Japan [27]. Apart from bitcoin and currencies, the amazing characteristics of blockchain are revealed in short by creating a transparent paper trail that anyone can access it but no one can alter it. Decentralization or shared control, immutability and native assets, have good impacts on existing technologies such as artificial intelligence and IoT. Thereby decoupling bitcoin of blockchain is a must, as bitcoin is just one application of many others that could be applied in different domains such as medical, Security, votes, games, art, scientific discoveries, intellectual properties, copyrights, etc. these technologies when combined with blockchain platform, they will change the near future dramatically and turn many science fictions into reality. Generally speaking, anywhere that a database can be used as a mean of storing information, a blockchain could be used in order to add a set of features to empower existing and future applications to be as useful as possible.

A. Central ledger vs Distribued Ledger vs Blockchain

To fight against single point of failure, the centralized systems use many approaches based on replication where ledger is maintained by a central authority (single place). It depends how information is distributed on a central ledger, where in general, normal users have limited access to the ledger so they can add or change records based on their predefined privilege. Access to the ledger enables them to add entries as well as read or change existing ones where security is applied to the ledger based on identity and integrity of those users. Domain name service (DNS) is a good example of central ledger. Any centralized system puts its effort on checking streaming data records that come into its database by building a complex system which is considered costly in terms of money and time.

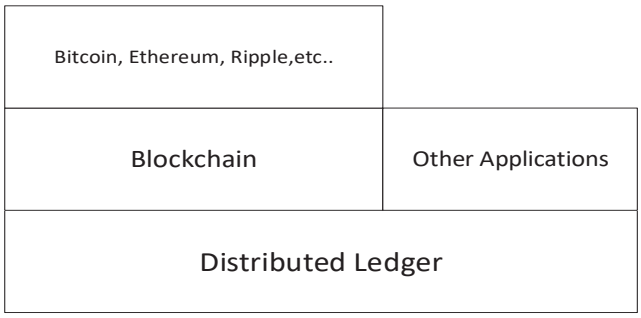

Figure 4: Distributed Ledger topology

On the other hand, distributed ledgers are designed to mainly fight against single point of failure as well as single point of control hence ledger is distributed equally to all peers in the network without relying on any authoritative copy, whereas it uses a consensus mechanism to prevent modification of an ordered series of time-stamped records. Distributed ledgers simplify the operations and minimize the fraud based on cryptographic verification instead of user identity. Centralized ledgers can also mitigate the risk of transactions being recorded differently. This is because all parties share the same records and can recognize the history of the transaction. Hashgraph [28] is a distributed ledger application that differs from blockchain by recording multiple transactions at the same time, rather than recording one transaction after another in a chain. Distributed ledgers improve relationships and efficiency in the businesses especially for a company which regularly deals with unknown or new customers. A blockchain is a type of a distributed ledger, comprised of unchangeable timestamps records by hashing them into an ongoing chain of hash-based proof-of-work, digitally recorded data in block of transactions that are validated by consensus mechanism based on the online data of distributed ledger. We can conclude that all blockchains are distributed ledgers, but not all distributed ledgers are blockchains (see figure 4).

B. Blockchain characteristics

First it is important to note that the distributed ledger is structured into two main network types:

- *Permisionless network:* such as bitcoin, where anyone can join the network without previous permission. Participants of this type can validate the transaction and might be part of the consensus and block creation.

❖ *Permissioned network:* this is a private network limited to a number of trusted entities that got permission to join the network in order to validate transactions. Microsoft recently deployed blockchain as a service called "Ethereum consortium blockchain" [33]. It consists of a set of load-balanced transaction nodes, with which an application or a user can interact to submit transactions and a set of mining nodes to record transactions.

- Apart of general ledger, blockchain is characterized by awesome features and benefits allowing blockchain revolution to change our lives. Below are the most advantage/characteristics of blockchain:

Transparency: per design, each peer in the network has a copy of the ledger therefore containing a full history of every transaction, enabling traceability of each asset back to its origin. Participants might be able to better understand the source of goods and services that they buy. This could allow more informed consumer decision making. Tracking each transaction within the chain is the fruit of this technology thus adding more benefits to businesses.

Decentralized system: Blockchain is a peer to peer network where peers are equal in terms of authority and rights. Central authorities are no longer existent in such system where rules and behaviors are predefined by the software itself. Obviously, eliminating the third party from any system, has a good impact on the organization budget where servers and some other hardware become useless. The bigger the network is, the more stable it is. Thus there is no worry about failure of some nodes since the ledger exists on many others.

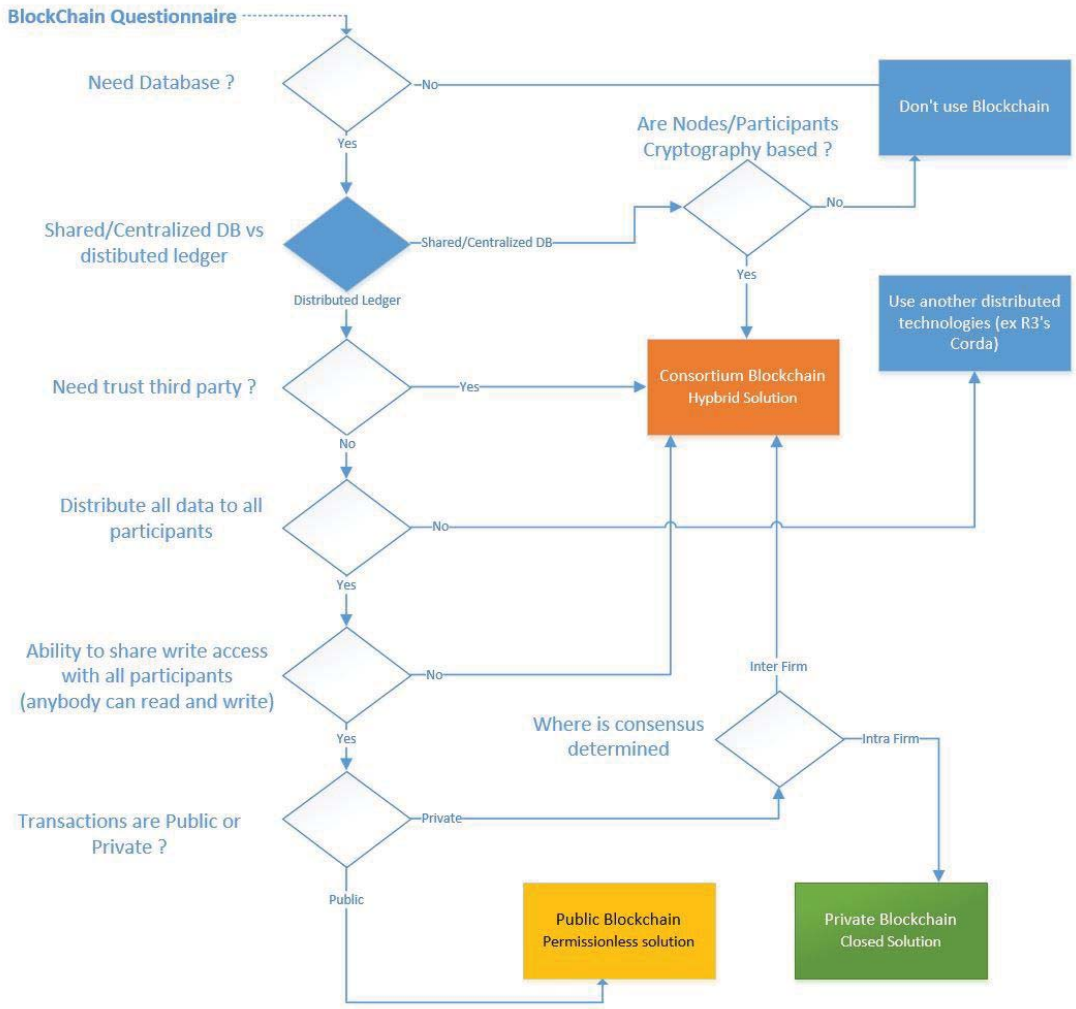

Figure 5: Blockchain varieties

Consensus: This is the main mechanism of a decentralized system that enables peer-to-peer value exchange without involving a trusted third party or intermediary for that consensus, by enabling the entire network to reach agreement about which blocks of transactions are valid and which ones are not There are different models of distributed consensus such as Proof of work that is used by bitcoin and aims to achieve agreement on its propagated transactions. Many other models such as proof of stake, proof of existence are suitable to be used in different scenarios rather than financial purpose.

Tamper-Proof: it is a distributed system mainly relying on cryptography system to maintain the whole network. Essentially, each participant in the network has its own private/public key. Public key is designed to be shared by everyone on the network while private should be kept by the participants. Each transaction is digitally signed using a participant's private encryption key and validated by its public key to ensure the transaction is created by the holder of that specific private key. A hash function is used thereafter to create a unique digital fingerprint for this transaction, which is then hashed with other transactions into a block. Once a block has been accepted by network, it is cryptographically bounded to the ledger and distributed to all the nodes. This block cannot be changed after its creation, a fact which renders the blockchain suitable for many use cases such as ownership registrations.

Smart Contract: it is integrated with blockchain second generation. The concept was first discussed in Nick Szabo's paper 1997 [32]. Basically, a smart contract is a computer code based on "if-then" condition where events are in direct relation to their contracts occurs, then actions are triggered to satisfy the smart contracts conditions. Ethereum is one of the cryptocurrency application that mainly relies on smart contracts. The integration of smart contract with blockchain eliminates the need for an intermediary and minimizes contractual-related transaction costs.

C. Blockchain Considerations

Blockchain with its characteristics listed above is considered flexible and suitable to replace many applications. Many use cases are now being explored in different fields other than financial and payments, including portfolio management reporting, product distribution, security and anti-fraud measures.

Three blockchain implementations could be used: i. the *public blockchain* is the most famous approach such as bitcoin where anybody can send transactions and expect to see them in the next block of the chain. Participants are involved in the verification process "consensus" and assisting in determining which transactions get added into the ledger and which are not.
ii. *Consortium blockchain* is considered a hybrid solution, however, it gives permission to some nodes to participate in the Consensus process. For example, a Central Bank allows only trusted Banks to provide the necessary controls and thus verifies transactions before adding them to the block. Furthermore, the read permission of the ledger can also be restricted. Accordingly, this type is often known as a partially-decentralised Blockchain. Finally, iii. the *Private Blockchain* type consists of one organization that has the permission to create (write) new transactions however the read permissions are restricted to only selected nodes. Private blockchain is probably used by management/auditors companies that need to control some sensitive activities which are measured internally, where public read access does not apply within their applications.
In Figure 5, we illustrate a questionnaire to help organizations for better using the blockchain feasibilities.

V. Conclusion

In this work, we introduced blockchain as an innovative technology used by the well-known cryptocurrency "Bitcoin". The success of bitcoin imposes the blockchain usage in large scales, thereafter thousands of applications based on blockchain are provisioned in the market in order to be totally or partially independent of the centralized systems. Blockchain as a distributed system nowadays represents a new application feature that replaces an existing client-server core system on top of some distributed systems with many additional features such as HA, resistance to alteration, fault tolerance and cost reduction. We also provided a questionnaire helping organizations for better using the blockchain feasibilities.
In the future work, we will investigate deeply the blockchain use cases, their impacts on socio-economy and treat them to rapidly involve this technology in the market.

VI. References

[1] N. Szabo, "Secure property titles with owner authority," 1998. https://nakamotoinstitute.org/secure-property-titles/

[2] S. Nakamoto. (2008, Nov.). Re: Bitcoin P2P e-Cash Paper [Online]. https://www.mailarchive.com/cryptography@metzdowd.com/msg09997.html

[3] A. Back, "Hashcash - a denial of service counter-measure," 2002. http://www.hashcash.org/papers/hashcash.pdf

[4] J. Turek and D. Shasha, "The many faces of consensus in distributedsystems," IEEE Comput., vol. 25, no. 6, pp. 8–17, Jun. 1992.

[5] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society,April 1980.

[6] D. Malkhi and M. Reiter, "Byzantine quorum systems," Distrib.Comput., vol. 11, no. 4, pp. 203–213, 1998.

[7] R. C. Merkle, "A digital signature based on a conventional encryption function," in Proc. 7th Conf. Adv. Cryptol. (CRYPTO'87), Aug. 1987,vpp. 369–378.

[8] H. Massias, X. S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirement," in Proc. 20th Symp. Inf. Theory Benelux (SITB'99), May 1999.

[9] B. Schoenmakers. Security aspects of the EcashTM payment system. State of the Art in Applied Cryptography, 1998.

[10] R. L. Rivest. Peppercoin micropayments. In Financial Cryptography,2004

[11] N. T. Courtois, "On the longest chain rule and programmed selfdestruction of crypto currencies," Computing Research Repository, Tech. Rep. abs/1405.0534, 2014.

[12] J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, and E. Wustrow, "Elliptic curve cryptography in practice," in Proc. 18th Int. Conf. Financial Cryptogr. Data Secur. (FC'14), Mar. 2014, pp. 157–175.

[13] D. Ron and A. Shamir, "Quantitative analysis of the full bitcoin transaction graph," in Proc. 17th Int. Conf. Financial Cryptogr. Data Secur. (FC'13), Apr. 2013, pp. 6–24.

[14] M. Fleder, M. Kester, and S. Pillai, "Bitcoin transaction graph analysis," Massachusetts Institute of Technology (MIT), Computer Systems Security, Tech. Rep. 6.858, 2013.

[15] G. Andresen, "BIP 16: Pay to script hash," Jan. 2012 [Online]. https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki

[16] J. Douceur, "The Sybil attack," in Proc. 1st Int. Workshop Peer Peer Syst., Mar. 2002, pp. 251–260.

[17] T. Bamert, C. Decker, R. Wattenhofer, and S. Welten, "Bluewallet: The secure bitcoin wallet," in *Proc. 10th Int.Workshop Secur. TrustManage.*, Sep. 2014, pp. 65–80

[18] G. Andresen, "BIP 11: M-of-N standard transactions," Oct. 2011. https://github.com/bitcoin/bips/blob/master/bip-0011.mediawiki

[19] S. Goldfeder, J. Bonneau, E. W. Felten, J. A. Kroll, and A. Narayanan, "Securing bitcoin wallets via threshold signatures," Tech. Rep., 2014.

[20] S. Goldfeder et al., "Securing bitcoin wallets via a new DSA/ECDSA threshold signature scheme," Tech. Rep., 2015

[21] V. S. Miller, "Use of elliptic curves in cryptography," in *Proc. 5th Conf. Adv. Cryptol.*, Aug. 1985, pp. 417–426.

[22] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.

[23] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," ACM Trans. Program. Lang. Syst., vol. 4, no. 3, pp. 382–401, 1982.

[24] H. Finney. (2011). Best Practice for Fast Transaction Acceptance—How High is the Risk. https://bitcointalk.org/index.php?topic=3441.

[25] Leslie Lamport. The part-time parliament. ACM Transactions on Computer Systems (TOCS), 16(2):133{169, 1998.

[26] M. H. F. Reid. An analysis of anonymity in the bitcoin system. In 2011 IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing, 2011.

[27] http://www.cnbc.com/2017/04/12/bitcoin-price-rises-japan-russia-regulation.html

[28] Wright, ping: Distributed ledgers are the future of identity security, TechTarget,http://searchcloudsecurity.techtarget.com/news/450303520/ Ping-Distributed-ledgers-are-thefuture-of-identity-security

[29] T. McConaghy, R. Marques, A. Muller, "BigchainDB: A Scalable Blockchain Database (DRAFT)". Berlin, 2016

[30] J. A. Kroll, I. C. Davey, and E. W. Felten, "The economics of bitcoin mining, or bitcoin in the presence of adversaries," in Proc.

[31] 2014 Bitcoin Developer Documentation [Online]. Available : https://bitcoin.org/en/developer-documentation

[32] N. Szabo, "The idea of smart contracts," 1997. http://szabo.best.vwh.net/smart_contracts_idea.html

[33] https://www.microsoft.com/developerblog/2018/02/26/ using-private-ethereum-consortium-network-store-validate-documents/